Department of the Army
First Region (ROTC)
United States Army Cadet Command
Fort Bragg, North Carolina 28307-5000

FRMOI 380-19
5 March 1999

Security

INFORMATION SYSTEMS SECURITY OFFICER ACCREDITATION HANDBOOK

FOR THE COMMANDER:

KERRY R. PARKER
COL, AD
Chief of Staff

PROPONENT: The proponent of this publication is Information Management Division, Headquarters, First Region (ROTC) US Army Cadet Command. Comments should be sent directly to Headquarters, First Region (ROTC), US Army Cadet Command, Fort Bragg, NC 28307-5000.

DISTRIBUTION: Distribution is determined by the proponent. Distribution codes used are explained in FRMOI 25-1.

SUPPRESSION: This is a new publication.

Distribution: A; D; S
This document is available on the World Wide Web at: **www-rotc.monroe.army.mil/firstregion**

This Information Systems Security Officer Accreditation Handbook updates any previous instructions provided to brigades and battalions. Significant changes include:

* Removal of the position/title of Terminal Area Security Officer to comply with national policies (AR 380-19).

* Simplified format.

****

NOTICE

- Take care to read ALL instructions completely.

- Forward a copy of all required accreditation documents to the First Region (ROTC) Information Management Division (IMD).

- Maintain on file a copy of all required accreditation documents.

- These instructions do not apply to privately owned systems. Privately owned systems may be approved for use on an exception basis only. Waiver must be approved by the First Region (ROTC) Information Systems Security Manager (ISSM).

GENERAL INSTRUCTIONS

1. The following guidance pertains to all computers (government and university) accredited under the provisions of this directive.

* Specific guidance is provided at the beginning of each example. It is important that all examples be used to ensure all security and administrative requirements are met.

* Failure to comply with all requirements outlined will result in a revocation of the computer's accreditation. Revocations of accreditation will be documented by the First Region (ROTC) IMD and forwarded through channels to the ISSO concerned.

2. The brigade or senior school commander is the Designated Approval Authority (DAA) and will sign and approve the Accreditation Document.

3. The DAA appoints an Information Systems Security Officer (ISSO) to:

* Properly safeguard the computers and information.

* Properly control the operation of the systems.

* Continuously observe the normal operation of the systems.

4. Systems approved at the Unclassified Non-sensitive and Sensitive but Unclassified Level are not authorized to communicate information to systems which have been approved to process classified data.

5. Communicating systems are generally operated in a dedicated (all users possess the same level of security clearance and same need to know) or system high (users have same level of security clearance and different need to know) security mode.

6. The Communications Security (COMSEC) waiver dated 5 Mar 98 must be included with the accreditation packet on file. The document is available on the First Region (ROTC) Website (**www-rotc.monroe.army.mil/firstregion**) on the **IMD** Page.

7. Accreditation under these procedures is finalized upon signature by the DAA and the responsible ISSO and forwarding of the required documents to First Region (ROTC), ATTN: ATOA-IM. No further approval is needed.

8. A complete Accreditation Packet consists of **ALL** of the following. The original accreditation packet must be retained by the organization ISSO and a copy of the items marked with * must be provided to First Region (ROTC), ATTN: ATOA-IM.

* Certification of Use/Accreditation Memorandum.

* One copy of each ISSO appointment memorandum.

* One current copy of List of Equipment for each computer.

* One copy of the current signed Security Briefing Record.

The COMSEC waiver.

The Automated Information System Security SOP.

The Risk Assessment modified for the organization.

9. The documents listed in paragraph 8 are available on the First Region (ROTC), World Wide Web Homepage, IMD Support Page for downloading and modification by the ISSOs. The COMSEC waver is a pdf file and cannot be modified.

ACCREDITATION MEMORANDUM

Instructions for the Accreditation Memorandum

a. The Accreditation Memorandum will be used in its entirety and signed by the DAA and ISSO.

b. Accreditation period for each computer is three (3) years from the date of signature by the DAA and the ISSO. In the event that the DAA or ISSO departs prior to the end of the three-year period, the succeeding DAA and/or ISSO will sign the current accreditation memorandum as the next succeeding DAA or ISSO. A copy of the updated memorandum and a copy of the appointment memorandum for the succeeding ISSO must be forwarded to First Region (ROTC) IMD. The brigade/battalion must maintain the original memorandum on file with the appointment memorandum for the succeeding ISSO.

c. The original of the Accreditation Memorandum will be retained by the organization ISSO and a copy will be provided to First Region (ROTC), ATTN: ATOA-IM.

LETTERHEAD

(Office symbol) Date

MEMORANDUM FOR Commander, First Region (ROTC), ATTN: ATOA-IM,
Fort Bragg, NC 28307-5000

SUBJECT: Certification of Use/Accreditation of Stand-Alone or Communicating Computer/Laptop Processing Unclassified Non-sensitive or Sensitive But Unclassified (SBU) Level Information

1. AR 380-19 requires Automated Information Systems that process Unclassified Non-sensitive or Sensitive but Unclassified Information be accredited to operate. Accreditation takes into account the risks associated with operating the computer in its office environment and the countermeasures taken to protect the information's confidentiality, integrity, or availability.

2. Purpose of this certification/accreditation is to ensure that unclassified sensitive information processed by the computer is:

a. Protected from disclosure to unauthorized persons.

b. Protected from destruction/alteration by hackers or other unauthorized personnel.

c. Protected from corruption or destruction by computer viruses.

d. Available, complete, and accurate for use by managers and operators when needed.

e. Protected by each operator who will comply with the security controls stated in paragraph 3 below and the governing Automated Information System Security SOP.

3. In accordance with AR 380-19, the computer system(s) identified within the attached List of Equipment as Stand-alone is/are accredited to process and store Unclassified Non-sensitive or Sensitive but Unclassified Information in the Dedicated Security Mode. The computer system(s) identified within the attached List of Equipment as Communicating is/are accredited to process and store Unclassified Non-sensitive or Sensitive but

Unclassified Information in the Systems High Security Mode. The following conditions are acknowledged, understood, and complied with by the computer operator(s) listed in the Record of Security Briefings at Appendix E. **(NOTE: The approved COMSEC waiver is required for the accreditation to be effective.)**

a. The processing and/or storage (includes transmission with or without a modem) of classified information on this system is prohibited.

b. The system will be used only for official government purposes.

c. Only software that has been specifically developed or approved for use or has been purchased or leased by an authorized U.S. Government representative and listed on the List of Equipment, will be used with this computer.

d. The operator will ensure the confidentiality of Privacy Act and For Official Use Only information by preventing unauthorized access to the computer equipment, media, and printed material.

e. The operator is responsible for the physical security of the computer and its associated equipment.

4. I, the undersigned, acknowledge and understand the conditions and responsibilities of operating the computer(s) identified in paragraph 3 above and will comply with all of the conditions.

Signature _____
(Typed Name & Title of ISSO) (Date)

Signature _____
(Typed Name & Title of Accreditation Authority (Date)

AUTOMATED INFORMATION SYSTEM SECURITY SOP

Instructions for AIS Security SOP.

a. This SOP will be reproduced and used in its entirety. A copy will be maintained by the organization ISSO.

b. All computer operators will read the AIS Security SOP and sign the Record of Security Briefing, Appendix E.

AUTOMATED INFORMATION SYSTEM SECURITY SOP

1. References:

a. AR 380-19.

b. Memorandum, US Army Cadet Command, ATCC-IMO, 5 March 1998, subject: Extension of Exception to Policy for Communications Protection.

2. Purpose:

a. To prescribe policy and procedure to ensure adequate personnel, physical, communications, electromagnetic emanations, hardware, software, procedural, and all other security aspects contributing to protection of stand-alone and communicating unclassified Automated Information Systems (AIS).

b. This SOP establishes procedures for stand-alone systems (including laptop computers) and networks. Stand-alone unclassified systems require the least amount of protection to meet the required level of security as prescribed by governing regulation. Networks require different methods of achieving the desired level of protection. This SOP is intended to outline minimum security standards required to adequately protect all stand-alone and communicating, unclassified automated information systems.

c. Situations involving conflicts between this SOP and other DOD/DA regulations and directives will be resolved in favor of those higher regulations. Users are reminded that this SOP provides only the minimum standards to be implemented. More stringent requirements may be implemented and are encouraged; however, less stringent safeguards may not be substituted.

d. All systems accredited/certified under the parameters of this SOP must comply with these standards before accreditation/ certification is finalized by the accreditation authority.

3. Objectives:

a. Safeguard sensitive defense information against espionage, sabotage, misuse, or compromise.

b. Protect computers (including laptop computers); sophisticated word processing equipment; software; and data from theft, misappropriation, damage and misuse.

c. Establish uniform security procedures for operation of unclassified stand-alone and networked AIS throughout First Region (ROTC).

4. Responsibilities:

a. Commanders:

(1) Serve as the DAA.

(2) Appoint Information Systems Security Officer (ISSO).

(3) Assume overall responsibility for the safeguarding of the AIS for which they endorse on the Accreditation Memorandum.

b. ISSOs: In addition to performing those duties outlined in Chapter 1, AR 380-19, the ISSOs will perform the following functions:

(1) Act as a primary point of contact for the system(s) charged to their responsibility.

(2) Ensure that an accreditation packet is prepared in accordance with this directive. Ensure that accreditation packets are approved prior to commencing AIS operations.

(3) Actively oversee the security of the system(s) for which they are charged.

(4) ISSOs are given authority under paragraph 1-6d(3), AR 380-19, to cause operations to be partially or completely suspended upon detection of any action which may affect the security of operations.

(5) Ensure personally owned computers are not used in the work place without prior approval of First Region (ROTC) IMD.

(6) Ensure only authorized software is allowed to be operated on AIS.

(7) Report all changes concerning the accreditation of the system(s) to First Region (ROTC) IMD.

(8) Notify the First Region (ROTC) IMD whenever possible compromises of classified information occur.

(9) Perform all other duties as required by pertinent regulations.

5. Security Controls:

a. Physical Security:

(1) Windows to the computer area are locked and secured at the end of the duty day. Windows that cannot be adequately locked are secured in one of the following manners:

(a) Metal security screening.

(b) Boarded/bricked windows.

(c) Windows above the first level (approximately 12 feet above ground level) and outside the perimeter of external stairways or fire escapes do not require additional security safeguards.

(2) Window air conditioners are screened or otherwise made to be capable of preventing their removal and serving as a means of entry to the computer area.

(3) Doors are reinforced to strengthen their normal physical construction (e.g., multiple locks, locking bars, welded hinges, etc.) when they serve as the sole means of access from the building exterior.

(4) Where possible, rooms/buildings housing computer systems are monitored after duty hours by security personnel on a regularly scheduled basis.

(5) All unclassified materials relating to the AIS are stored in one of the following:

(a) Locked desk.

(b) Locked file cabinet.

(c) Locked independent office.

(d) Any other locking container which affords double barrier protection.

(6) Each system is marked in a manner that provides a permanent means of rapid identification. This will be done for each component of the system. These markings will:

(a) Identify the equipment as being the "PROPERTY OF THE U.S. GOVERNMENT." The term "ARMY" may be substituted for "GOVERNMENT."

(b) Be either engraved, branded, or written with an identifiable, traceable agent.

(c) Be placed in a manner that can be readily inspected and is readily visible when installed in its normal operating position.

(7) All AIS, located in areas where personnel other than the authorized users possess access, are secured by one of the following measures during non-duty hours when left unattended:

(a) Locking cabinet.

(b) Locks and security cables.

(c) Lock-down pads.

(d) Security personnel.

b. Access Control and Security:

(1) The use of locking keyboards/CPUs and/or passwords is used to deny unauthorized personnel access to the information and operation of the AIS.

(a) Keys and/or passwords are issued to users and controlled by the ISSO.

(b) Passwords are changed semiannually. A record is maintained for issue of passwords by the ISSO.

(c) Passwords generated by the ISSO or system administrator are issued to only one user.

(d) Workstations and desktop computers should include a local “idle lockout/screen saver” feature that automatically locks the screen and keyboard after a specified period of no activity requiring reauthentication before unlocking the system. Programming and instructions are available on the First Region (ROTC), World Wide Web Homepage, IMD Support Page.

(2) Only personnel with a need to know who are properly briefed on system safeguards will be allowed use of the AIS.

(3) All AIS media (hard drives, diskettes, tapes, printouts, etc.) is provided protection IAW:

(a) AR 340-17 (Privacy Act information)

(b) AR 340-21 (For Official Use Only information)

(4) Custodial personnel who clean computer areas after duty hours are escorted or closely monitored. Checks are made of computer areas after departure of these personnel. In those cases where no security personnel are present overnight to supervise custodial personnel, the ISSO will require users to conduct pre-operation inspection to identify:

(a) Tampering.

(b) Unauthorized access.

(c) Theft.

(5) Maintenance personnel required to provide service for processing systems will be escorted at all times. Whenever possible, processing systems should remain within the operational area. In the event that systems must leave the operational area, the ISSO must ensure the proper safeguarding of sensitive information prior to release of the equipment. This will be accomplished by:

(a) When possible, overwrite non-removable storage devices/media IAW procedures outlined in Appendix B, AR 380-19. BACKUP ALL REQUIRED DATA/PROGRAMS PRIOR TO DELETING OR REFORMATTING THE DEVICE(S).

(b) If storage media is removable, provide the media appropriate storage until return of the repaired equipment.

c. Environmental Security:

(1) Fire extinguishers are made available for emergency use. The location of fire equipment is made known to all users of the system. Non-water extinguishers are available to protect the users and equipment.

(2) AIS are not placed in areas where damage from flooding, falling objects, excess heat or electrical hazards is likely to occur.

(3) AIS are left uncluttered and given adequate air circulation to prevent overheating and reduce fire hazards.

(4) Eating, drinking and smoking in the immediate area of AIS is prohibited.

(5) AIS are located away from open windows, sunlight, radiators, and heating vents.

(6) AIS and peripherals located in areas exposed to excessive dust and microscopic particle pollution are covered and disk drive doors closed when not in use.

(7) AIS are located on stable desks or tables.

(8) Surge suppressors or uninterrupted power supplies are used on all systems to protect AIS from electrical power fluctuations.

d. Personnel Security:

(1) Although not required, personnel possessing security clearances will be verified and monitored by the ISSO. Security investigations are performed on personnel occupying ADP I, II, and III positions, although security clearances may not be required. The ISSO coordinates with the First Region (ROTC)

Security Manager and other involved offices regarding the integrity and character of operator personnel. Users of all systems are monitored by the ISSO to ensure their trustworthiness concerning the security of the system(s).

(2) Initial security briefings will be presented to all personnel to ensure that they are familiar with the security provisions of the Automated Information System Security SOP. Each user will acknowledge that they understand these security procedures by signing an acknowledgment sheet at Appendix E.

e. Communications Security: Transmission security devices are not required for stand-alone computers. The requirements for communicating computers outlined in reference 1a above requires the use of approved communications security devices for the transmission of unclassified sensitive information. The availability of these devices is extremely limited for the protection of unclassified information. Until such time as the capability exists to encrypt all required unclassified transmission, the following countermeasures are to be implemented:

(1) Log outs. AIS are logged out when left unattended for any period of time.

(2) Passwords. As applicable, passwords used by network system users/operators are issued to an individual and are not to be shared. Users will memorize their passwords and destroy printed copies. These passwords are not to be stored in the vicinity of the system. Issuance of a password constitutes a license for that individual to operate.

(3) Remote devices connected to the system are afforded the same safeguards listed above as the host/mainframe.

(4) All data is to be transmitted using Terminal Server Access Control System (TSACS) IAW reference 1b above.

f. Emanations Security: Emanations security is not a factor for unclassified sensitive systems.

g. Procedural Security:

(1) Users are trained on the use of software programs prior to commencing actual operations to prevent the destruction/damage of data.

(2) Users are not allowed editing capabilities of system and application executable files within a network. This serves as a means of minimizing destruction/damage of files and the introduction of viruses.

(3) Users are allowed access to system and application files as required. This access will be restricted to the maximum extent possible as a means of minimizing destruction/damage of files and the introduction of viruses.

(4) Users will ensure that proper start up and shut down procedures are known and followed.

(5) Backup copies of data files are performed on a daily basis. These backups are stored separately from the system(s).

(6) AIS are configured so as to provide a screen indicating the level of processing authorized on the system whenever the start up procedure is initiated or whenever a user logs on to the system. Screen messages are available from the First Region (ROTC) IMD. Programming and instructions are available on the First Region (ROTC) World Wide Web Homepage, IMD Support Page.

(7) Privacy Act/FOUO data is controlled, stored, disseminated, and destroyed IAW AR 25-55 and AR 340-21. Recipients of this data are informed of protection requirements.

(8) Privacy Act and FOUO data is destroyed by shredding or, as a minimum, tearing/cutting data into four pieces.

(9) Users will not reproduce government owned software for use on more than one system at a time, unless it is a multi-user software package. Government owned software will not be used for private use or personal gain.

(10) Users conduct end-of-day checks to ensure:

(a) That the user is logged out.

(b) That all sensitive items have been properly stored/destroyed.

(11) All diskettes are scanned by users for virus programs prior to being processed on any AIS. Diskettes are scanned both initially and whenever users lose absolute control

of diskettes that have been utilized on another system. This includes all program, application, and data diskettes.

(12) Users are instructed not to use government AIS for the playing of computer games. Users are informed that they can be disciplined for improper utilization of these systems.

h. Software Security:

(1) Original copies of operating and application software are secured under separate lock and controlled by the ISSO to deter theft. The ISSO will establish and maintain a complete inventory of all software holdings. Software will be inventoried semiannually by the ISSO. Records of these inventories are maintained by the ISSO and are subject to inspection.

(2) Only the ISSO may grant authority to load authorized software on government systems. The ISSO will personally supervise the loading process. NO GAMES WILL BE LOADED ON GOVERNMENT COMPUTERS except those games included in government purchased software used in training purposes.

(3) Locally produced software will be approved by the ISSO prior to being installed on any AIS.

(4) The anti-virus software available on the First Region (ROTC) Web Homepage will be installed on all computer equipment used to support the First Region (ROTC) mission. Incidents where a virus is detected will be reported to First Region (ROTC) IMD.

6. Users of systems governed by this SOP will be required to read and document in writing their understanding of this SOP on the Record of Security Briefing at Appendix E.

ADDITIONAL DUTY APPOINTMENT MEMORANDUM

OFFICE SYMBOL Date

MEMORANDUM FOR See Distribution

SUBJECT: Additional Duty Appointment

1. Effective (DATE), (NAME), (SSAN), is appointed as Information Systems Security Officer for the (ORGANIZATION).

2. Authority: AR 380-19.

3. Purpose: To comply with the provisions of AR 380-19.

4. Period: This appointment will remain effective until rescinded.

5. Special Instructions: Comply with referenced publication in the performance of your duties.

Signature Block
Commander/PMS

DISTRIBUTION:

1 Accreditation Packet
1 ATOA-IM
1 Individual designated

RECORD OF SECURITY BRIEFING

I acknowledge that I have read and understand the requirements outlined within the Automated Information System Security SOP. I further acknowledge my responsibilities for the safeguarding, disseminating, storing, and destruction of materials and equipment related to the computer system(s) concerned.

NAME	DATE	SIGNATURE

NOTE:

1. Original copy of the form will be maintained by the organization ISSO. One copy will be provided to First Region (ROTC) IMD.

2. All personnel will be briefed on Automated Information System Security on an annual basis.

EQUIPMENT LIST

Instructions for Equipment List.

a. Complete and maintain one form for each computer being accredited. Maintenance of this sheet will eliminate the need for numerous surveys in the future.

(1) When equipment is exchanged for maintenance, the List of Equipment will be updated by lining through the old serial number and adding the new serial number. Provide a copy of the updated page to the First Region (ROTC) IMD promptly.

(2) When new equipment is received, update the appropriate page or create a new page for new systems. Provide a copy of this page to the First Region (ROTC) IMD promptly.

b. **Category**: There are three categories of computers. The ISSO must determine the correct category for each computer. The categories are:

- **Stand-Alone Computer**

- **Communicating Computer**

- **Communicating Laptop**

(1) Stand-alone computers are those AIS that do not communicate or transfer information to another AIS through the use of data/telephone/radio links. Stand-alone computers possess all equipment and components necessary to process, view, enter/retrieve, and print data/information. In addition to previously mentioned criteria, all of the following conditions must exist for computers accredited under stand-alone category:

* AIS is that type which is referred to as a "desk top" or "personal (not privately owned) computer" (PC).

* AIS is designed for use by one individual at a time.

* AIS is not used at any time for communicating information nor for processing classified information.

* System is operated in a dedicated security mode (all users possess the same level of clearance and same need to know).

* This category may be used when accrediting desktops and laptops with **modems that are not used**, and are processing unclassified information. Be sure to identify on the List of Equipment that the modem is either inoperative/not used/or that the computer is not used for communications purposes.

(2) Communicating computers or laptops are those AIS that communicate or transfer information to another AIS through the use of data/telephone/radio links. These systems may consist of:

* Networked Local Area Network/Wide Area Network (LAN/WAN) systems.

* Small systems incorporating dumb/smart terminals or desktop/PCs.

* Dial-up/point-to-point systems.

Accreditation processed under this format must identify:

* The specific network (e.g., University network, TSACS, etc.) in which the system is operating.

* All anticipated or known communication uses of the system(s).

c. **Make/Model**: i.e., AST 486, DELL Pentium.

d. **Hard Drive Capacity**: i.e., 700MB, 2.5GB

e. **Amount of RAM**: i.e., 16MB, 32MB

f. **Processor Speed**: i.e., 90MHz, 200MHz

EQUIPMENT LIST

Category: _____
HARDWARE
CPU Serial Number: _____
Make/Model: _____
Hard Drive Capacity: _____
Amount Of RAM: _____
University or Government Owned: _____
Processor Speed: _____
PERIPHERALS
List equipment name and serial number for each peripheral. (monitor, printer, scanner)

Equipment Name	Serial Number

SOFTWARE

Title	Version No.	University or Government Owned

Communicating Laptop or Desktop Info:

1. Does this system have a modem in use? YES _____ NO _____
2. Is the system used for:
   a. Point to point communications? YES _____ NO _____
   b. Within the University Network? YES _____ NO _____
   c. Within the TSACS network? YES _____ NO _____
   d. Within the Army Standard Information System (ASIMS)? YES _____ NO _____
3. Communications from this computer will be secured during transmission by:
   a. Other Type 1 or 2 encryption device? YES _____ NO _____
   b. Software encryption? YES _____ NO _____
   c. COMSEC waiver YES _____ NO _____

ISSO NAME/RANK	SCHOOL NAME

Instructions for Risk Analysis

This a sample Risk Analysis. ISSOs must modify the sample document to accommodate their risk management program IAW AR 380-19, Chapter 5.

Letterhead

Office Symbol Date

MEMORANDUM FOR Information Systems Security Officers (ISSOs)

SUBJECT: Risk Analysis for Automated Information Systems (AIS) Processing Unclassified Non-sensitive and Sensitive But Unclassified (SBU) Level Information

1. Purpose. The purpose of the Risk Management Review is to conduct a detailed review of the risks associated with the user operation of computer systems to process Unclassified Non-sensitive and Sensitive But Unclassified level information. The information developed as a result of this Risk Management Review will be used by Information Systems Security Officers (ISSOs) in the accreditation process for computer systems within their activity. This formal risk analysis satisfies the requirements of Chapter 5, AR 380-19.

2. Objective. The objective of risk management is to achieve the most effective safeguards against deliberate or inadvertent:

a. Unauthorized disclosure of information.

b. Denial of service or use.

c. Unauthorized manipulation of information.

d. Unauthorized use.

3. Methodology. The four steps used to conduct this review are: threat identification, vulnerability analysis (VA), risk assessment (RA), and countermeasures (CM). Definitions of the terms are as follows:

a. Threat Identification. A description of the threat and threat agent as they relate to specific security areas, e.g., physical security, personnel security, etc.

b. Vulnerability Analysis (VA). Indicates the probability of a threat occurring and provides the rationale used in calculating the probability. Probabilities are addressed as high, medium, or minimal.

c. Risk Analysis (RA). This is a determination of the anticipated losses that would result from a threat that is carried out to completion.

d. Countermeasures (CM). Identification of existing and proposed actions that are designed to provide a deterrent to the opportunity of a threat or serve to minimize the loss if the threat is carried to completion.

4. Analysis and Assessment. The review in this section is divided into the recognized automation security sub-disciplines of physical, communications, emanations, hardware, software, personnel, and procedural security. A definition of each sub-discipline precedes the review of that area.

a. Physical Security. Physical security is provided to computer systems through the application of barriers and procedures of the protected area. Physical access controls will be established to deter unauthorized entry into the computer. Physical access to magnetic media (floppy diskettes, backup tapes, etc.) will be controlled. The effects of disasters such as fire and flood will be prevented, controlled, or minimized by the use of fire extinguishers and through the use of backup tapes stored off-site.

(1) Threat. A fire originating in an office area.

VA. The probability of a fire originating in a building constructed of masonry is minimal, especially in light of the requirement to use fused power line protection (surge protectors) and the DoD Smoking Only in Designated Areas policy. However, the threat of a fire originating in a wooden building is high, due to old, faulty or overloaded wiring, lighting, etc.

RA. A fire in an office area would threaten the entire office. All equipment and software would be exposed to extensive smoke or water damage or total destruction.

CM. All organizations shall periodically prepare back up disks/tapes and store them off-site at another location. Additionally, ISSO should consider negotiating a mutually supporting Continuity of Operations Plan (COOP) with other organizations that have like hardware. Fire inspections shall be conducted IAW fire regulations. The fire safety program in wooden buildings shall be increased to ensure awareness of potential fire hazards.

(2) Threat. Water damage from plumbing.

VA. The probability of water damage to a computer system due to a broken water pipe in a masonry building is minimal, except in basement areas where it is medium. The probability of water damage to a computer system due to a broken water pipe/rain leaking through the roof in a wooden building is high due to the deteriorating age of the building.

RA. A broken water pipe or rain leaking through the roof would pose an electrical shock hazard to personnel and damage the hardware if water were to make contact with the system. Power shut down would deny the use of the system.

CM. Where possible automated systems shall not be placed directly under plumbing pipes. In areas where overhead pipes are located or in wooden buildings where an automated system is located adjacent to a window or other area likely to leak, periodic inspections shall be made for evidence of developing leaks and plastic sheeting should be readily available to cover the equipment. All personnel shall know where the master power switch is located.

(3) Threat. A flood.

VA. The probability of a flood occurring on the installation is minimal due to its geographic location and the drainage of the general area.

RA. A flood would not pose a significant threat.

CM. Facility engineers have the capability of removing accumulated water resulting from a greater than average rainfall.

(4) Threat. Commercial power failure.

VA. The probability of a commercial power loss is medium and is a definite threat.

RA. The loss of commercial power poses a problem in that it contributes to the loss of magnetic media files.

CM. The cost of providing emergency backup power to all systems is not economically feasible based on the numbers of systems processing unclassified non-sensitive or sensitive but unclassified information. Key locations are provided with power backup or line stabilizers that allow an orderly power down without the loss of information. Automated systems which are essential to the activity/unit shall use an uninterrupted power supply (UPS).

(5) Threat. A mechanical failure of air conditioning system.

VA. The possible loss of the air conditioning system during the summer months is medium. Normal wear and tear is expected. Spare air conditioning systems are probably not immediately available. Some computer systems are located in not air conditioned areas.

RA. An extended loss of the air conditioning system during the summer months could result in the shut down of the computer systems. Systems located in facilities not air conditioned may have to shut down during periods of the day. The mission of the activities/units would be impaired due to the shut down of the system.

CM. Facility engineers are on call and are available to repair air conditioners within a reasonable time. Activities/ units not having air conditioned areas should consider shifting operational times to early morning/late evening periods.

(6) Threat. Severe thunderstorm/lightning strikes resulting in damage to utility lines, buildings, and equipment.

VA. The possibility of the loss of utilities, facilities, and equipment is medium.

RA. Losses would result in a shut down of information processing.

CM. Emergency repairs would be undertaken immediately. Units/activities having essential information processing requirements should consider activation of a COOP plan or

relocation to another area not affected by the loss of power. Where warning of imminent danger exists, AIS must be turned off or unplugged to reduce possibility of damage.

(7) Threat. Major windstorm damage to buildings/ equipment.

VA. The possibility of a major windstorm in the area is high. Major damage in a masonry building is minimal. Major damage to a wooden building is high.

RA. Major damage to buildings could shut down operations.

CM. Immediate repairs and reroute of communications traffic would begin within a short time after the damage. Alternate work locations would be selected. Implement COOP operations as soon as possible.

(8) Threat. Earthquake resulting in the destruction of buildings.

VA. The threat of an earthquake is minimal and, if one did occur, it is unlikely that it would be of the magnitude necessary to produce structural damage.

RA. A major earthquake would cause total disruption of operations.

CM. Activation of a COOP plan should be considered.

(9) Threat. An intruder/vandal found on site with intent to destroy.

VA. The probability of an intruder/vandal attempting to gain access with intent to destroy is minimal, except in wooden buildings where the probability is medium.

RA. Intrusion could be expected to cause damage to the equipment and software.

CM. Automated systems which process unclassified non-sensitive and sensitive but unclassified information and have an internal hard drive must employ some form of access control, e.g., a software security system which requires a password to

gain entrance or a physical lock over the power switch. These systems shall also have two barriers. For example, two separate locks:

- One on an outer door and one on an inner door.

- Or one on an outer door and a locking cable on the computer system.

(10) Threat. An intrusion of security areas with intent to gain information.

VA. The probability of intrusion for the purpose of gaining information is minimal.

RA. Intrusion could be expected to cause the loss of Privacy Act, For Official Use Only and other similar material.

CM. All visitors should be escorted to prevent unauthorized intrusion.

(11) Threat. An intruder found on site with intent to introduce false data into the programs.

VA. The possibility of an intruder attempting to introduce false data or information is minimal.

RA. False data could cause the unit/activity a large amount of damage or lost time.

CM. Access to automated systems shall be controlled. All personnel introducing information into the systems shall be required to provide positive identification. Briefings will be conducted regularly on acceptance procedures. All personnel introducing information into the system will use only approved software and follow established procedures.

(12) Threat. An intruder/vandal gaining access to the hardware and software with the intent to destroy.

VA. The probability of an intruder/vandal attempting to gain access for the purpose of destruction of the system is minimal due to the generally smaller size of the system (versus a larger, more costly computer system) and due to the large quantity of systems.

RA. The destruction of the operational programs would cause a minimal delay in processing.

CM. Positive ID of all visitors is mandatory prior to granting access to the spare operational programs.

(13) Threat. A theft of computer systems, and/or theft of internal components.

VA. The possibility of the theft of a desktop or laptop computer or internal components is very high based on their portability, ease of converting to private use, or sale.

RA. The loss of the unit's/activity's computer system would have an adverse affect on the mission. The loss of an internal component might prevent the unit/activity from accomplishing a needed function.

CM. Current directives require that computers be permanently marked with the serial number and the words "Property of the US Government." When this policy is applied, the risk of theft is reduced due to the much higher risk to the thief knowing that stolen equipment can be traced and identified. Attempting to remove the markings would leave damage to the case so that its value for sale would be significantly reduced. Fort Bragg Label 43 identifies the equipment as Army property that has been marked with a traceable, invisible ink for ready identification by law enforcement personnel.

b. Communications Security. Automated systems that communicate or network with other systems are required to employ some form of protection for Privacy Act, For Official Use Only, and other unclassified non-sensitive and sensitive but unclassified transmissions. This protection can include the use of Type 1 encryption devices, Data Encryption Standard (DES) equipment, or the use of a Protected Distribution System (PDS).

(1) Threat. Unauthorized monitoring of data communications links.

VA. The possibility of this type of unauthorized monitoring being used to gain information is minimal. However, modern methods of monitoring systems would make unauthorized monitoring relatively simple.

RA. The monitoring of data transmissions and information being processed on computer systems could compromise the data since few systems use encryption devices or PDS protection.

CM. Systems which transmit unclassified non-sensitive and sensitive but unclassified information should be protected by encryption or through the use of a PDS whenever possible.

(2) Threat: Unauthorized hacking into AIS with intentions of stealing information, destroying data files and inserting malicious codes.

VA. The possibility of this type of unauthorized entry into computer system is highly likely due to the abundant hacker programs available off the Internet. Today's hackers need not be a highly educated computer analyst, but only able to download the hacker's software programs, and most times at no cost. Additionally, due to the manpower shortage, most system administrators cannot devote the time to continually monitor the system for anomalies.

RA. Breaking into computer system is relatively easy due to the huge number of unprotected networks and availability of hacking software.

CM.

(1) Installation of firewalls can block IPs and prevent hackers from identifying sensitive information about the system and its users.

(2) Installation of IDS can monitor computer systems being accessed and in identifying authorized access attempts.

(3) System Administrators and Network Managers should be trained on identifying and using C2 Protect tools.

c. Emanation Security. This area of protection is provided through the use of TEMPEST approved equipment and installation considerations for systems which process classified information. Since this risk management covers only unclassified processors, risk assessment of this section is not required.

d. Hardware Security.

(1) Threat. Unauthorized persons posing as maintenance personnel with the intent of copying data, altering programs or destroying hardware systems.

VA. The possibility of this type of threat is unlikely due to the high risk of being discovered.

RA. A loss of the hardware and software systems would impair the office/unit that had been penetrated. Total disruption of the system could be effected.

CM. Maintenance personnel shall be escorted and under visual observation at all times.

e. Software Security. This area of protection is provided through government purpose/application programs, and routines that protect data and hardware of an AIS system and its resources. Additionally, government directives establishes mandatory policy on use of software.

(1) Threat. Unauthorized changes to application or executive programs either intentional or unintentional.

VA. The possibility of this type of threat is unlikely because the software for automated information systems and communication terminals are standard off-the-shelf items.

RA. A change to the operational programs would cause a loss of control for the processing of information until a new diskette could be created.

CM. Only authorized personnel will be allowed to change computer configuration, and modify/delete software. Original copies of applications software must be maintained.

(2) Threat. Theft of software for unauthorized uses.

VA. The possibility of this threat is likely due to the high cost of some system software which could be applied to home computers.

RA. Loss of the system software would have an adverse effect on the mission if the system were to crash. A loss of time would result attempting to locate and re-install another copy of system software.

CM. The periodic unannounced and spot checks conducted by the unit ISSO act as a deterrent to such crime. Supervisors must be knowledgeable of the threat of this type of crime.

f. Personnel Security. Personnel security is the area of protection and procedures established to ensure that all personnel who have access to sensitive defense information have the required authority as well as the background investigation.

(1) Threat. Disloyal personnel with the intent to provide information to unauthorized persons.

VA. The probability of this type of threat is unlikely. The material processed on these systems is Privacy Act, For Official Use Only, and other similar sensitive information. This Risk Analysis does not cover classified processors.

RA. The loss that would result from this type of threat could be considered minimal.

CM. ISSOs must conduct the initial screening and investigation of personnel prior to allowing them to work as a computer operator. Suspicious acts by coworkers should be reported.

(2) Threat. Disgruntled employees whose intent is to disrupt operations by destroying operational programs or falsifying information input/output.

VA. The probability of this type of threat is possible and in some cases likely as a way to get back at supervisors or the unit/activity.

RA. The manipulation of the operational programs would cause a minor disruption of operations and mission until a new disk could be created or retrieved from storage. Falsification of information in the unit or office area would cause confusion within the mission area. Recovery of the false information could cause a minimal delay in mission execution if discovered in time.

CM. Daily observations and/or removal of disaffected operators and regular reviews of information systems and software will minimize the chances for introduction of false information. Supervisors who maintain an open channel of communication with their employees and who become actively engaged in the problem

solving process will greatly reduce the possibility of disgruntled employee damage. Personnel that are being considered for disciplinary action/removal from service should be removed from duties as a computer operator/programmer.

(3) Threat. Human error resulting in a loss of data through erroneous processing.

VA. The possibility of this type of unintended loss is likely due to the complexity of some operations and lack of operator training.

RA. The loss of data through human error would cause a minimal delay of operations due to the need to retrieve the information from backup storage. On-line transmission and reception of information would not be impaired.

CM. Ensuring proficiency through the use of training programs. Observation of newly assigned personnel by supervisors is made mandatory during performance of sensitive operations. Spare diskettes with backup information must be stored for contingency purposes.

(4) Threat. The loss of key personnel due to transfer, retirement, or emergency leave.

VA. The possibility of this type of loss is likely due to the complexity of the command and the turnover and loss of personnel.

RA. The loss of personnel due to transfer would cause minimal problems due to constant cross training of personnel and use of the backup system of duty assignments. Mission impairment would be minimal.

CM. Constant cross training of all personnel, presence of written guidance such as a SOP/MOI, and backup assignment of tasks and missions will ensure minimal interruption.

g. Procedural Security. Procedural security is the area of protection provided by management constraints. Operational, administrative, and supplemental controls are established to provide protection for the data or information.

(1) Threat. Operators unintentionally processing classified information on a system accredited only for unclassified operation.

VA. This type of threat is likely in offices where both classified and unclassified processing occurs.

RA. Classified information unknowingly placed in a unclassified environment increases the potential for its compromise.

CM. ISSOs must train operator personnel to recognize classified information (which has been properly marked), so that information will not be processed on the unclassified processor. Supervisors must be educated to assure that they do not task an operator to process classified on an unclassified processor. Spot checks by security personnel will help ensure compliance.

5. Findings. The level of risk associated with the operation of automated systems within this organization has been evaluated. Considering the security measures in place and/or passed, the operation of these systems under present security standards is within acceptable limits.

6. Advice And Assistance. This formal risk analysis satisfies the requirements of Chapter 5, AR 380-19 and applies to all unclassified computers within this organization.

Signature of the
Accreditation Authority